استخدام شبكة القبعة المكسيكية Mexican Hat Net في زيادة سرية النص المشفر

مها عبد الإله محمد البدراني
قسم هندسة البرمجيات / كلية علوم الحاسبات والرياضيات
جامعة الموصل

الاستلام ٢٦ / ٠٦ / 2008 القبول ١٦ / ٠٢ / ٢٠٠٩

ABSTRACT

The interactive with information considers a large problem specially in transformation of information that need a top security and storage.

Therefore, it was necessary using the artificial neural network ,that consider from the modern application in artificial intelligent, if it dependent on biological bases in simulation human behavior.

This search dependent on the idea of cipher by the use of decimated alphabet cipher and for the purpose of increasing the security of cipher data ,the feed is done on the artificial neural network, which is the (Mexican Hat Net) to enter the cipher text for the purpose of increasing the security of the text and then decipher.

The result provide the ability of ciphering by using the decimated alphabet cipher method with Mexican Hat Net and then decipher and checked the correct of the results in the operation of decipher keeping on the security of these cipher data from hackers by this algorithm.

الملخص

تعد عملية التعامل مع المعلومات في بعض الأحيان مشكلة كبيرة، وخصوصاً في نقل المعلومات التي تحتاج إلى السرية التامة والخزن لذلك كان من الضروري التوجه إلى الشبكات العصبية الاصطناعية التي تعد من التطبيقات الكفوءة في مجال الذكاء الاصطناعي، إذ اعتمدت على أسس بيولوجية في محاكاة السلوك البشري.

تم في هذا البحث اعتماد فكرة التشفير باستخدام الشفرات الهجائية العشرية ولغـرض زيادة أمن البيانات المشفرة تم تغذية الشبكة العصبية الاصطناعية وهي شبكة القبعة المكسيكية بإدخالات النص المشفر لغرض زيادة أمن النص المشفر ومن ثم فك شفرته.

برهنت النتائج إمكانية التشفير باستخدام طريقة الشفرات الهجائية العشرية مع شـبكة القبعة المكسيكية ومن ثم فك الشفرة والتأكد من صحة النتائج في عملية فك الشفرة من خـلال الحفاظ على أمن البيانات المشفرة من الاختراق بهذه الخوارزمية.

١. المقدمـة

احتلت سرية المعلومات أهمية كبيرة منذ أقدم العصور وازدادت أهميتها مع تقدم العلوم حيث لا ينكر احد مدى أهمية التشفير لاسيما مع انتشار قراصنة الانترنت وسرقة المعلومات في كل أنحاء العالم، إن الاحتياج لتحسين امن البيانات والمعلومات في أنظمة الحاسبات الالكترونية هو نتيجة مباشرة للاستخدام المتزايد للحاسبات في معالجة وخزن وإيصال البيانات القيمة والحساسة.

ويمكن النظر للمعلومات بصفتها بيانات تمت معالجتها لجعلها مفيدة وان المصطلحين (بيانات ومعلومات) غالباً ما يكونون متطابقين، فالأمن والسرية تعني حماية البيانات والمعلومات بحيث تكون [7] :

١. غير قابلة للتحوير.
٢. غير قابلة للتحطيم.
٣. غير قابلة للإفشاء.

إن إخفاء المعلومات المفيدة في صورة غير مفهومة هو الحلم الذي حققه علم التشفير (Cryptology) وهو عبارة عن مصطلح يطلق على التشفير وتحليل الشفرة، طرائق التشفير يمكن استخدامها لحماية البيانات والمعلومات من الإفشاء المغرض او التلقائي إن الشبكات العصبية الاصطناعية (Artificial neural networks) تعرف على أنها نماذج رياضية لمعالجة المعلومات تقوم بمحاكاة شبكة عصبية حيوية للحصول على شبكة عصبية اصطناعية[8].

وتعد شبكة القبعة المكسيكية Mexican Hat Net إحدى الشبكات العصبية الاصطناعية التي تتميز بقدرتها على التكييف والتعديل عن طريق التعلم لإنتاج قرار معين حسب طبيعة المسألة المراد حلها[7].

٢. التشفير

إن خوارزمية التشفير (Encryption Algorithm) عبارة عن خوارزمية تستخدم لتحويل الرسائل الى صيغة سرية باستعمال حروف تعويضية محل الحروف الأصلية أو بواسطة تبديل موضع الحروف للرسالة الأصلية، تعمل خوارزمية التشفير بالاشتراك مع المفتاح لتشفير النص الصريح (Plain Text)[1] .

النص الصريح (Plain text) هو الرسالة الأصلية التي يمكن قراءتها، المفتاح (Key) عبارة عن معادلة او وسيلة استخدمت بواسطته عملية التشفير أو الترميز، أما النص المشفر (Cipher text) فهو الشكل المشفر للرسالة، اما خوارزمية فك التشفير (Decryption Algorithm) عبارة عن خوارزمية يتم فيها إرجاع الرسالة المشفرة الى شكلها الطبيعي(النص الصريح) [8] .

والشكل (١) يوضح مراحل التشفير وفك التشفير :

الشكل (١): يوضح مراحل عملية التشفير وفك التشفير

٣. خوارزميات التشفير

هناك خوارزميتان أساسيتان للتشفير وهما[8]:

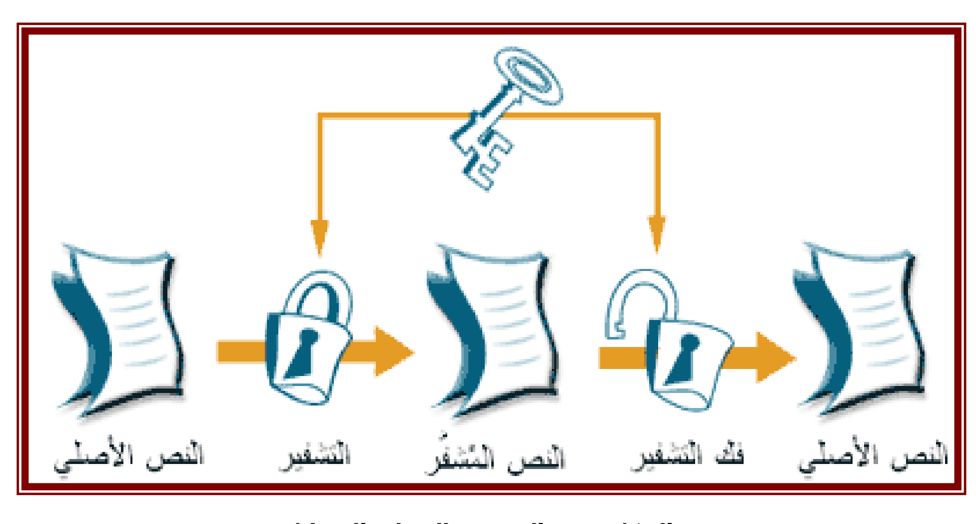
١) التشفير بالمفتاح المتناظر (Symmetric key cryptograph) أو المتماثل.

٢) التشفير بالمفتاح غير المتناظر (A symmetric key cryptograph) أو اللا متماثل.

1.3. التشفير بالمفتاح المتناظر

في التشفير المتماثِل (Symmetric key cryptograph) يستخدم كل من المرسِل والمستقبِل المفتاح السري ذاته في تشفير الرسالة وفك تشفيرها ويتفق الطرفان في البداية علـى عبـارة المرور ((pass phrase) كلمات مرور طويلة) التي سيتم استخدامها، تُحول عِبارةَ المرور إلى عدد ثنائي، ويتم إضافة رموز أخرى لزيادة طولها ويشكل العدد الثنائي الناتج مفتاح تشفير الرسالة[7].

وبعد استقبال الرسالة المشفرة، يستخدم المستقبِل عبارةَ المـرور نفسها من أجل فك شفرة النص المشفر (Cipher text or Encrypted text)، إذ تُترجِم البرمجيـات مـرة أخـرى إلى عبارةَ المرور لتشكيل المفتـاح الثنائـي (binary key) الذي يتولى إعادة تحويل النص المشفر إلى شكله الأصلي المفهوم والشكل (٢) يوضح طريقة التشفير بالمفتاح المتماثل:

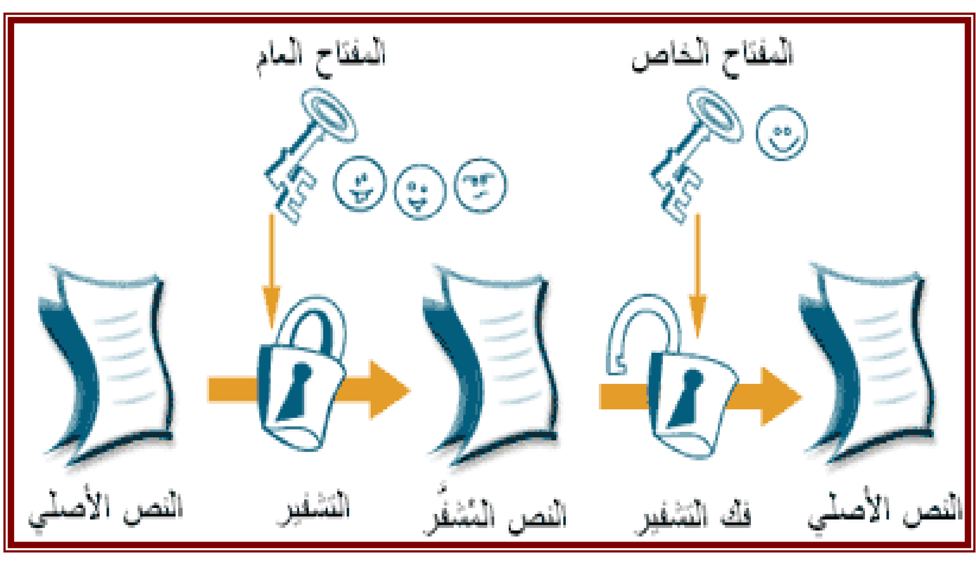


الشكل (٢): التشفير بالمفتاح المتماثل

2.3. التشفير بالمفتاح غير المتناظر

جاء التشفير اللا متماثل (A symmetric Key Cryptograph) حلاً لمشكلة التوزيع غير الآمن للمفاتيح في التشفير المتماثل، فعوضاً عن استخدام مفتاح واحد، يستخدِم

التشفير اللا متماثِل مفتاحين اثنين تربط بينهما علاقة ويدعـى هذان المفتاحان بالمفتاح العام (public key) والمفتاح الخاص (private key) يكون المفتاح الخاص معروفاً لدى جهـة واحـدة فقط أو شخص واحد فقط وهو المرسِل، ويستخدم لتشفير الرسالة وفك شفرتها أما المفتاح العام فيكون معروفاً لدى أكثر من شخـص أو جهـة، ويستطيع المفتاح العام فك شفرة الرسالة التي شفرها المفتـاح الخاص، ويمكن استخدامه أيضاً لتشفير رسائل مالـك المفتـاح الخاص، ولكن ليس بإمكان أحد استخدام المفتاح العام لفك شفـرة رسالة شفرها هذا المفتاح العام، إذ إن مالك المفتاح الخاص هو الوحيد الذي يستطيع فك شفرة الرسائل التي شفرها المفتاح العام[8]. والشكل (٣) يوضح طريقة التشفير بالمفتاح اللامتماثل:



الشكل (٣): التشفير بالمفتاح اللامتماثل

٤. التشفير التعويضي (Substitution Cipher)

في هذا النوع من التشفير المتماثل ينتج النص المشفر(Cipher text) عن طريق استخدام رموز (Symbols) معينة، كل رمز من هذه الرموز يمثل كلاماً يفهمه الطرف الأخر المتلقي للنص المشفر، كما ينتج النص المشفر (Cipher text) من خلال التعويض عن كل كلمة- أو حرف مكون لكل كلمـة- مـن كلمات النص (Plain text) المهم الذي نرغب فـي حمايته بقيمة عددية تمثل نمط معين مستخدم في حياتنا، كالتعويض عن كل حرف بما يقابله من قيمته العددية في جدول وهو نظام الترميز القياسي الأمريكي لتبادل المعلومات (ASCII -American Standard Code for Information Interchange) أو إزاحة الأحرف بمقدار معين يطلق عليه المفتاح (Key)، وينتج في نهاية الأمر نصاً ليس له معنى ولا يوجد ترابط بين محتواه.

هذا النوع من التشفير يعد أفضل لأنه يجعل النص الصريح (Plain text) يصبح ذا أمنةً (Security) أكبر، ولهذا النوع عدة طرق مختلفة نذكر أهمها[8]:

١. شفرة مورس (Morse Code)
٢. شفرة قيصر (The Caesar Cipher)
٣. الشفرات الهجائية العشرية (Decimated Alphabet Cipher)
٤. أنظمة تشفير الاسكي (ASCII Cipher Systems)
٥. الشفرات الرقمية (A Number Cipher)

٥. الشفرات الهجائية العشرية

لضمان توفير أمنية عالية يتم اعتماد هجائية تستخدم مفتاحاً يقوم بتوفير الإزاحة ولكن بشرط أن تكون الأحرف فيها ذات تسلسل غير متتابع مثل هذه الأبجدية من الممكن توفيرها بواسطة نظام الشفرة الهجائية(Decimate Cipher System)[8] .

إن عملية التشفير باستخدام طريقة الشفرات الهجائية العشرية يتطلب استخدام مضاعف لغرض توليد الهجائية العشرية بدلاً من إضافة المفتاح، ولغرض توضيح التسلسل الغير متتابع للشفرة العشرية عندما k=3 كالأتي:

النص الصريح	A	B	C	D	E	F	...	U	V	W	X	Y	Z
رقما	1	2	3	4	5	6	...	21	22	23	24	25	26
النص المشفر	C	F	I	L	O	R	...	K	N	O	T	W	Z
رقما	3	6	9	12	15	18	...	11	14	17	20	23	26

الإزاحة من حرف إلى حرف غير ثابتة:
A إلى C = 1 إلى 3
B إلى F = 2 إلى 6
Y إلى W = 25 إلى 23

إن نمط الأحرف غير متتابع وهجائية المشفر تتألف من كل حرف ثالث من هجائية النص الصريح.

٦. شبكة القبعة المكسيكية

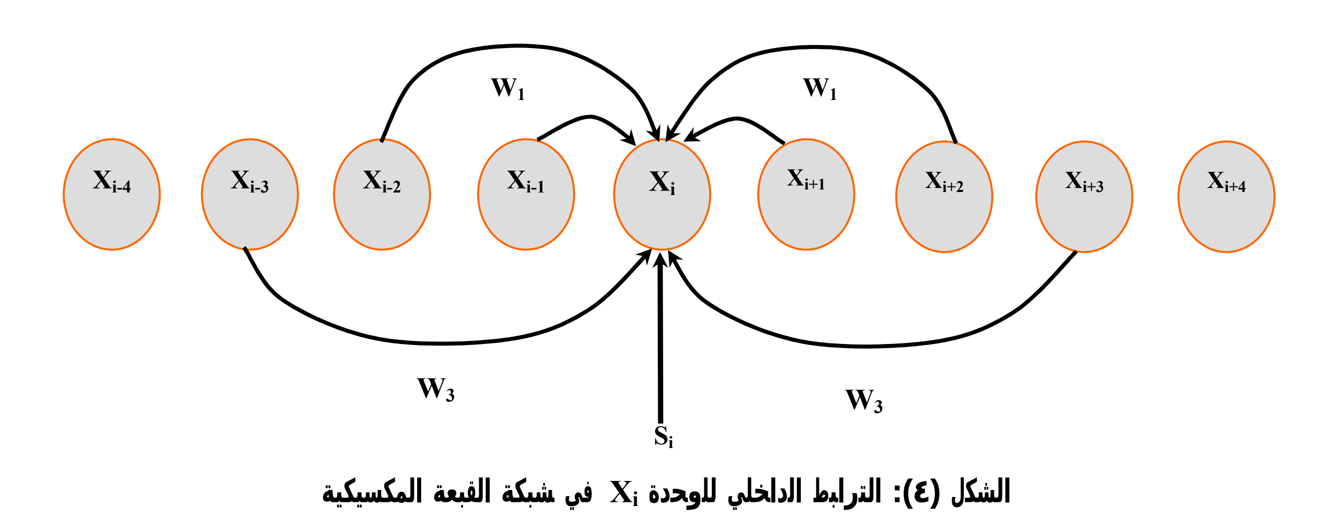
اقترح شبكة القبعة المكسيكيـة (Mexican Hat Net) العالم (Kohonen) في عام (1989)، وهي من الشبكات العصبية الاصطناعية الأكثر انتشاراً في الشبكـات الفرعيـة المعتمدة على مبدأ تعاظم التباين، حيث يتم ربط كل عصبون من عصبونات الشبكة بروابط محددة (وبأوزان موجبة) مع عدد من العصبونات القريبـة للعصبون المركزي[2]، على حين

يملك كل عصبون أوزان ترابطات سالبة يمنع تعلمه ويكون مرتبطاً مع "جيران متنافسة" بعيدة عن العصبونات المركزية، وقد يكون بعض عصبونات الشبكة البعيدة لاتملك أي ترابطات مع عصبونات أخرى، وجميع هذه الترابطات تكون في طبقة خاصة، فإذا ما استقبلت العصبونات المركزية إشارة خارجية فضلاً عن إشارات ترابط داخلية، إذ يتم توليد عينة، اعتماداً على عينة الترابطات الداخلية، ووفق مراحل تكرارية للوصول إلى عينة الترابط الداخلي للوحدة xi .[3][5]

ومن اجل سهولة الوصف، فإن الوحدات المتجاورة تُصور كأنها مرتبة بطريقة خطية، ووفق ترابطات موجبة بين الوحدة xi والوحدات المتجاورة بأوزان موجبة، ووفق ترابطات سالبة من اجل الوحدات المتنافسة، ويختلف مجال الترابطات الموجبة والسالبة من مسألة إلى أخرى[2] [4].

٧. معمارية شبكة القبعة المكسيكية

تشمل الترابطات الداخلية لشبكة القبعة المكسيكية مجالين متناظرين حول كل عصبون مستقل[٦]حيث تكـون قيم أوزان الترابطـات الأقرب للعصبون المركزي أي بين الوحدة النظامية x_i والوحدات x_{i-2}،x_{i-1}، x_{i+2}، x_{i+1} موجبة وغالباً تؤخذ بنفس القيمة ويعبر عنها بالرمـوز W_1، W_2، على حين تكون قيم الأوزان بين الوحدة المركزية x_i والوحدات x_{i+3}، x_{i-3} فهي قيم سالبة ويعبر عنها بالرمز W_3، ولا يكون هناك أي ترابط بين الوحدة x_i والوحـدات x_{i+4}، x_{i-4} وبعبارات أخـرى نقول إن علاقة كل وحدة مركزية xi مع الوحدات المتجاورة بمسافة تمثل (d) فإذا كانت (d=1) و(d=2) بمعنى ان الوحدة المركزية xi ترتبط بأوزان موجبة، وعندما(d=3) فان الوحدة المركزية xi سوف ترتبط بأوزان سالبة وعندما (d>3) بمعنى الوحدة المركزية xi لا ترتبط بأي أوزان مع أي وحدة والشكل الأتي يوضح الترابط الداخلي للوحدة x_i [١٠] [٩]:



الشكل (٤): الترابط الداخلي للوحدة X_i في شبكة القبعة المكسيكية

٨. الجانب العملي للبحث

تم في هذا البحث استخدام خوارزمية شبكة القبعة المكسيكية (Mexican Hat Net) بعد إجراء عملية تشفير النصوص الانكليزية باستخدام طريقة الشفرات الهجائية العشرية (Decimated Alphabet Cipher) وذلك لزيادة سرية النص المشفر ومن ثم فك شفرة النص الذي تم تشفيره، والبحث يتضمن خوارزميتين رئيسيتين هما:

1.8 خوارزمية شبكة القبعة المكسيكية المستخدمة في زيادة سرية النص المشفر:

تتضمن خطوات عملية التشفير للنص الانكليزي الذي تم إدخاله باستخدام طريقة الشفرات الهجائية العشرية ومن ثم تغذية الشبكة العصبية الاصطناعية (شبكة القبعة المكسيكية) بإدخالات النص المشفر وذلك لغرض المحافظة على سرية النص المشفر من الاختراق.

الرموز المستخدمة في الخوارزمية هي:

- R_1: نصف قطر منطقة الترابطات الداخلية، حيث أن الوحدة x_i مرتبطة مع الوحدات $K = 1,\ldots\ldots, R_1$, x_{i-k} , x_{i+k}
- R_2: نصف قطر مجال الترابطات ذات الأوزان الموجبة $R_2 < R_1$.
- W_k: الوزن على الترابطات الداخلية بين الوحدات x_i , x_{i-k}, x_{i+} $_k$ حيث
- W_k قيمة الوزن الموجبة من أجل $0 \le k \le R_2$.
- W_k قيمة الوزن السالبة من أجل $R_2 < k \le R_1$.
- X: شعاع التنشيط.
- x_old: شعاع التنشيط الناتجة في خطوة الزمن السابقة.
- t_max: العدد الكلي للتكرارات من اجل تعزيز التباين.
- S: الإشارة الخارجية.

تقوم الخوارزمية الاتية بمطابقة الإشارة الخارجية المعطاة S فقط من اجـل التكـرار (خلال خطوة تدريب واحدة) من خطوات تكرارات تعزيز التباين وفق الخطوات الآتية:

١) تهيئة المعاملات t_max , R_1 , R_2 كما هو مطلوب، وتهيئة الأوزان وفق الشكل:

$W_k = C_1$ for $k = 0 \ldots\ldots, R_1 (C_1 > 0)$

$W_k = C_2$ for $k = R_1+1, \ldots\ldots, R_2\ (C_2 < 0)$

تهيئة x_old بقيمة صفرية.

٢) اخذ كل حرف من حروف الأبجدية الاعتيادية (A, B, C, ……, Z) واستبداله بالقيمة العددية التي تقابله: A =1, B = 2, …………, Z = 26

٣) أخذ القيمة التي حصلنا عليهـا في الخطوة (٢) وضربها بقيمة مفتاح التشفير (Key cipher)، المفتاح ممكن أن يأخذ أي قيمة عددية وترية بشرط أن لا تكون (13) أو احد مضاعفاتها (.... ,26, 52) لكي لا تكون القيمة الناتجة قيمة سالبة.

٤) القيمة التي حصلنا عليها في الخطـوة (٢) نقوم بتقسيمها على العدد (26.1) ونأخذ الجزء الصحيح من ناتج هذه العملية- عملية القسمة- (.........,0, 1, 2, 3).

٥) الجزء الصحيح الذي حصلنا عليه في الخطوة (٤) نقوم بضربه بالعدد (26).

٦) ناتج الخطوة (٥) تتم عملية طرحه من ناتج الخطوة (٢) ولتوضيح الخطوات من الخطوة (٢) إلى الخطوة (٦) نفرض ان :

a = القيمة العددية لاحرف الهجائية الاعتيادية.

K = قيمة المفتاح ويساوي ٣ .

k*a/26.1 = b

c = القيمة العددية لأحرف الهجائية العشرية.

حرف النص الصريح	القيمة العددية a	(K=3) K*a	b =k*a/26.1	C=ka-b(26)	حرف الهجائية العشرية
A	1	3	0.115	3	C
B	2	6	0.230	6	F
X	24	72	2.759	20	T

٧) تقديم شعاع الدخل الخارجي S، ووضعه بالشكل X = S، وتخزين شعاع التنشيط في المصفوفة: x_old for (i = I ....m)

بالشكل: $x_old_i = x_i$

اجعل عداد التكرار مساوياً للقيمة t = 1.

٨) طالما أن (t) لا يزال أقل من t_max نفذ الخطوات من 9 ⟵ 13.

٩) احسب دخل الشبكة من أجل i = 1.........., n بالعلاقة:

$$x_i = C_1.\sum_{k=-R_i}^{R_1} x_old_{i+k} + C_2.\sum_{k=-R_2}^{-R_1-1} x_old_{i+k} + C_2.\sum_{k=-R_1-1}^{R_2} x_old_{i+k}$$

١٠) طبق تابع التنشيط (تابع خطي يتدرج من 0 ⟵ X_max، بميل = 1).

$x_i = \min (x_max, \max (0,x_i)); (i = 1,.........., n)$

١١) أخزن التنشيطات الحالية في المصفوفة x_old.

$x_old_i = x_i \ (i = 1,.........., n)$

١٢) قم بزيادة عداد التكرار t = t+1.

١٣) اختبر شرط التوقف.

إذا كان $t < t_max$ استمر بالتعلم، وإلا توقف.

2.8. خوارزمية فك شفرة النص المشفر

تبدأ عملية فك الشفرة للنص الانكليزي المشفر باستخدام شبكة القبعة المكسيكية (Mexican Hat Net) من خلال اعتماد الخوارزمية الآتية:

١. تهيئة قيم R1, R2 والتي تمثل نصف قطر منطقة الترابطات الداخليـة، وR2 والتـي تمثل نصف قطر مجال الترابطات ذات الأوزان الموجبة، وW_k قيمة الوزن الموجبـة من أجل $0 \le k \le R_2$، و W_k قيمة الوزن السالبة من أجل $R_2 < k \le R_1$.

٢. x_old: شعاع التنشيط الناتج في خطوة الزمن السابقة.

٣. حساب معكوس المصفوفة x_old يتم من خلال توفر القيمة العددية للـنص المـشفر وقيمة الأوزان السالبة والموجبة.

٤. حساب اخراجات الشبكة والتي تمثل القيم العددية للنص المشفر.

٥. حساب معكوس طريقة الشفرات الهجائية العشرية وذلك بإتباع الخطوات مـن الخطـوة (٦) إلى الخطوة (٢) من خوارزمية شبكة القبعة المكسيكية المستخدمة في زيادة سـرية النص المشفر.

٦. تمثلت اخراجات خوارزمية فك شفرة النص المشفر بالقيم العدديـة الـصريحة للـنص الأصلي.

٩. البرمجيات وواجهات العرض المستخدمة في البرنامج

يتطرق البحث إلى بيان البرمجيات الخاصة بشبكة القبعة المكسيكية المـستخدمة فـي زيادة سرية البيانات المشفرة وكذلك فك شفرة النص المشفر، وكذلك إدراج النتائج التـي تـم الحصول عليها من تنفيذ هذه البرمجيات وذلك من خلال الواجهات.

تتألف البرمجيات المستخدمة في هذا البحث من برنامجين رئيسين (برنامج خوارزميـة شبكة القبعة المكسيكية المستخدمة في زيادة سرية النص المشفر) و (برنامج خوارزميـة فـك شفرة النص المشفر) ومجموعة من الدوال المبرمجة والتي تُنفذ ضمن البرنامجين الرئيـسين عند استدعائها. تم استخدام لغـة البرمجة المرئية (Visual Java) في كتابة برمجيات البحث لتنفيذ العمليات الحسابية والمنطقية، وكذلك تصميم واجهات عرض مناسبة للمستخدم لأغراض إدخال البيانات ومعرفة النتائج، فمن خلال الواجهة الرئيسة لبرنامج خوارزمية شـبكة القبعـة المكسيكية المستخدمة في زيادة سرية النص المشفر يتم إدخال البيانـات المـراد تـشفيرها وإدخال مفتاح التشفير وأوزان الشبكة، وتتم فيها عملية تشفير البيانات المدخلة والحصول على ناتج هذه العملية في نفس الواجهة وكما في الواجهة الآتية:

الشكل (٥): يمثل الواجهة الرئيسية

تحوي هذه الواجهة على مجموعة من الأزرار يمكن تلخيص وظيفة كل زر بالاتي:

١) **زر (Cipher):** يستخدم لتنفيذ عملية تشفير البيانات المدخلة.

٢) **زر (New):** يستخدم من أجل إعادة تهيئة البرنامج من جديد وذلك بإلغاء البيانات المدخلة ومفتاح التشفير وأوزان الشبكة وكذلك ناتج عملية التشفير الذي حصلنا عليه.

٣) **زر (Cipher display):** يستخدم هذا الزر لإظهار الواجهة التي تحتوي على ناتج عملية التشفير عند استخدام خوارزمية شبكة القبعة المكسيكية المستخدمة في زيادة أمن البيانات المشفرة، وكما في الواجهة الآتية:

الشكل (٦): واجهة عرض نتائج التشفير

٤) زر (Network Shape)

يستخدم هذا الزر لإظهار واجهة شكل شبكة القبعة المكسيكية المستخدمة في هذا البرنامج، وكما في الواجهة الآتية:

الشكل(٧): واجهة شكل الشبكة

اما برنامج خوارزمية فك شفرة النص المشفر باستخدام شبكة القبعة المكسيكية فيتم وفق الخوارزمية المذكورة سابقاً وبطريقة معاكسة لبرنامج خوارزمية شبكة القبعة المكسيكية المستخدمة في زيادة سرية النص المشفر.

١٠. الاستنتاجات

1.10 تأثير قيمة الوزن الأول والثاني للشبكة على البيانات الخارجة منها

إن قيمة الوزن الأول والوزن الثاني للشبكة تكون محددة بشرط معين وهذا الشرط هو أن تكون قيمة الوزن الأول للشبكة والذي يرمز له بـ (W1) اكبر دائما من الصفر ويمثل قيم الأوزان الموجبة أي:

$W1 > 0$

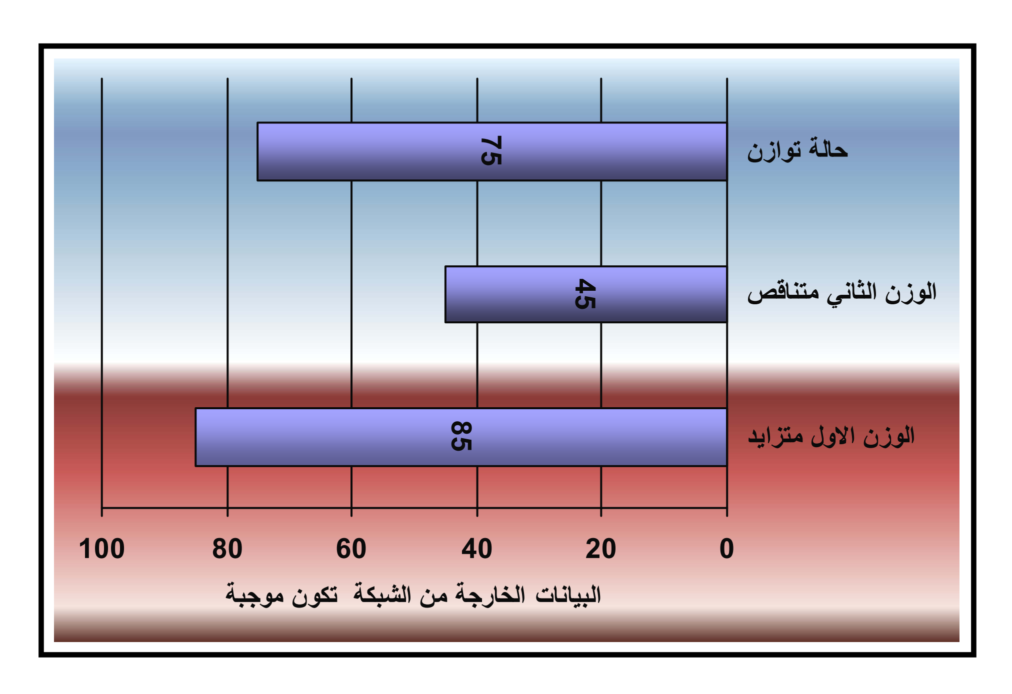
أما قيمة الوزن الثاني للشبكة والذي يرمز له بـ (W2) فيجب أن تكون دائماً اقل مـن الصفر أي:

$W2 < 0$

فلو كانت البيانات المدخلة إلى الشبكة هي ناتج تشفير الجملة (Neural Network) والتي هي (7 2 19 17 8 15 16 10 3 2 11 15 16)، فان القيم الخارجة من الشبكة سوف تكون مختلفة ومتغيرة باختلاف وتغيير قيمة كل من الوزن الأول والثاني للشبكة، الجدول(١) والشكل (٧) يوضحان ذلك:

الجدول (١): يمثل تأثير قيمة الوزن الأول والثاني للشبكة على البيانات الخارجة منها

W1	W2	Output Data from the Net
1	-1	20 40 9 -9 -12 12 30 12 5 27 23 11 -10 5
2	-1	51 82 37 7 3 41 71 51 45 71 61 39 -1 12
1	-2	9 38 -10 -34 -39 -5 19 -15 -30 10 8 -6 -29 3
2	-3	29 78 -1 -34 -51 7 49 -3 -25 37 31 5 -39 8
3	-5	38 116 -11 -77 -90 2 68 -18 -55 47 39 -1 -68 11
6	-6	120 240 54 -54 -72 72 180 72 30 162 138 66 -60 30
10	-7	233 604 147 -15 39- 171 333 201 155 231 275 161 -43 56
4	-9	25 150 -59 -161 -138 -37 65 -87 -155 23 -41 -135 10
7	-4	173 286 120 12 -3 135 243 165 140 240 206 128 -13 41



الشكل (٨): يمثل النسبة المئوية للبيانات الخارجة من الشبكة

من خلال الجدول والشكل السابقين نستنتج ما يلي:

١) كلما كانت قيمة الوزن الأول والثاني قريبة من الصفر سواء بالاتجاه السالب أو الموجب كلما كان هناك توازن في القيم الناتجة من حيث كونها قيم سالبة أو موجبة.

٢) إذا كانت قيمة الوزن الثانـي متناقصة بالاتجـاه السالب فان اغلب القيم الخارجة من الشبكة تكون عبارة عن قيم سالبة.

٣) إذا كانت قيمة الوزن الأول متزايدة بالاتجاه الموجب فان القيم الخارجة من الشبكة تكون قيم موجبة في أغلبها.

١١. أسباب استخدام شبكة القبعـة المكـسيكية وخوارزميتهـا فـي زيـادة أمنيـة البيانات المشفرة

إن استخدام هذه الخوارزمية في زيادة أمنية البيانات المشفرة يرجع للأسباب التالية:

١) مدخلات هذه الشبكة لا تكون عشوائية بل ناتجة من خوارزمية معينة استخدمت لتوليد هذه القيم.

٢) الشبكة تمثل نوع من أنواع الشبكات العصبية المبنية على التنافس (Neural networks based on competition)، ويكـون التنافس فـي هذه الشبكـة على أشده في المركز ويضعف عند الأطـراف، كما أن هذه الشبكـة تعتبر مـن الشبكات الوحيدة الطبقة (Single layer) وهذا يعني أنها لا تمتلك طبقات مخفية (Hidden layers)، بل تتكون من وحدات إدخال ووحدات أخراج، أيضا هذه الشبكة يكون طور التدريب (Training phase) فيها بدون إشراف (Unsupervised Training)، وهذا معناه أن الشبكة تتكون من متجه إدخال (Input vector) وخوارزمية تدريب (Training algorithm) لتغيير أوزان الشبكة لإنتاج متجه الإخراج (Output vector).

المصادر

١) الحمامي، أ.د علاء حسين، العاني، د. سعد عبد العزيز، "تكنولوجيا أمنيـة المعلومـات وأنظمة الحماية"، الطبعة الأولى، (٢٠٠٧)، دار وائل للنشر.

2) Droulez, J., & Berthoz, A. (1991). A neural network model of sensoritopic maps with predictive short-term memory properties. *Proc. Natl. Acad. Sci. U.S.A., 88*, 9653– 9657.

3) Hamaguchi, K., & Aihara, K. (2004). Quantitative information transfer through layers of spiking neurons connected by Mexican-hat type connectivity. *Neurocomputing,58–60*, 85–90.

4) J. P. L. Hatchett, (2006), "Analytic solution of neural network with disordered lateral inhibition", Department of Complexity Science and Engineering, University of Tokyo, Kashiwanoha 5-1-5, Kashiwa, Chiba, 277-8561, Japan and PRESTO, JST, Japan_Received 23 November 2005; published 4 May 2006_

5) Nowotny, T., & Huerta, R. (2004). "Explaining synchrony in feedforward networks". *Biol. Cybern., 89*, 237–241.

6) Okada, Masato, "Correlated Firing in a Feedforward Network with Mexican-Hat-Type Connectivity". (2000), Department of Complexity Science and Engineering, University of Tokyo, Kashiwa, Chiba, 277-8561, Japan; and Intelligent Cooperation and Control, PRESTO, JST, Shibuya-ku, Tokyo, 151-0065, Japan okada@k.u-tokyo.ac.jp

7) Ritter, Terry., (2007), “Ritter's Crypto Glossary and Dictionary of Technical Cryptography", All Rights Reserved. http://www.ciphersbyritter.com/LEARNING.HTM

8) S. Vanstone,(1996), "Handbook of Applied Cryptography", CRC Press. For further information, see www.cacr.math.uwaterloo.ca/hac

9) V. P. PLAGIANAKOS, “Global Search Methods for Neural Network Training”, Department of Mathematics, University of Patras Arti_cial Intelligence Research Center, e-mail: fvpp,gsa,vrahatisg@math.upatras.gr URL: www.math.upatras.gr/~vrahatis

10) Yazdanbakhsh, A., Babidi, B., Rouhani, S., Arabzadeh, E., & Abbassian, A. (2002), “New attractor states for synchronous activity in synfire chains with excitatory and inhibitory coupling”, *Biol. Cybern., 86*, 367–378.